



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/287,654	04/07/1999	PATRICK W. DOWD	DOWD-3-3	6548

27973 7590 06/25/2003

OFFICE OF THE ASSOC. GEN. COUNSEL (IP & T)  
9800 SAVAGE ROAD SUITE 6542  
FORT MEADE, MD 20755-6542

EXAMINER

REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 06/25/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)	
	09/287,654	DOWD ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) Responsive to communication(s) filed on 27 March 2003.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) Claim(s) 1-26 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 1,4-8,14 and 17-21 is/are rejected.

7) Claim(s) 2,3,9-13,15,16 and 22-26 is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) The proposed drawing correction filed on \_\_\_\_\_ is: a) approved b) disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12) The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some \* c) None of:

1. Certified copies of the priority documents have been received.

2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.

3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) The translation of the foreign language provisional application has been received.

15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_.

4) Interview Summary (PTO-413) Paper No(s) \_\_\_\_\_.

5) Notice of Informal Patent Application (PTO-152)

6) Other: \_\_\_\_\_.

Art Unit: 2131

## **DETAILED ACTION**

### ***Response to Arguments***

1. Applicant's arguments filed on March 27, 2003 have been fully considered but they are not persuasive. It is argued by the applicant that filtering is not the same as rules, the examiner respectfully disagrees. It is disclosed in the Microsoft Computer Dictionary that filter is defined as "a pattern or mask through which data is passed to weed out specified items" as recited on page 197. Rules is defined in Merriam Webster's Collegiate Dictionary as "to exist in a specified state or condition" as recited on page 1024. The examiner has found equivalence between the definitions of the two whereby the filtering of Descasper et al is a specific form of rules.

It is additionally argued that "Descasoer et al accepts every packet and makes no judgement concerning acceptability as do Applicants" and "Descasper et al does not mention a match for the purpose of determining whether or not to grant access to a packet." The examiner agrees with the applicant, but it is noted that the examiner has determined this limitation not to be taught by Descasper et al whereby the examiner has recited in the rejection "The teachings of Decasper et al are silent in disclosing of a disapproved list which contains information on connectionless packets which should be discarded. It is disclosed by Coley et al of monitoring incoming IP (connectionless) packets and to determine the validity of the source address (col. 8, lines 1-3 and col. 11, lines 47-48)." The teachings of Descasper et al is not relied upon for

Art Unit: 2131

teachings of comprising a disapproved list which contains information on connectionless packets which are to be discarded, but rather Coley et al is relied upon for this feature.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1,4-8,14, and 17-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Decasper et al in view of Coley et al.

As per claims 1 and 14, it is disclosed by Decasper et al of monitoring IPv6 (connectionless) packet whereby an association identification unit or AIU (database) stores information pertaining to a flow of data (connectionless) data packets and additionally stored filter information (rules). A received IPv6 (connectionless) packet is associated with an identifier (flow tag). If the (connectionless) packet includes an unknown flow, a new flow entry is automatically created (computed) for it which is added to and stored in the AIU (database comprising an approved list) and it is allowed to pass (pg 4 & 5). On pg 4 it is recited that the AIU (database) is used for flow detection which the examiner asserts that incoming identifiers (flow tags) are compared to (approved) data previously stored whereby a match is performed and the IPv6 (connectionless) packet is allowed to pass. It is inherent that teachings of Decasper et al initialize

Art Unit: 2131

the AIU (database) since it is necessary for relationships and data types are defined beforehand so that queries and manipulation of the data can be accomplished more efficiency. The teachings of Decasper et al are silent in disclosing of a disapproved list which contains information on connectionless packets which should be discarded. It is disclosed by Coley et al of monitoring incoming IP (connectionless) packets and to determine the validity of the source address (col. 8, lines 1-3 and col. 11, lines 47-48). If the analyzed source address is compared against authorized (approved list) and unauthorized (disapproved list) addresses maintained by a proxy agent (which is stored in a database) and the comparison includes checking if the source is unknown, if it is not on the list, then it is denied (col. 11, lines 22-32). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply a means of discarding unauthorized information that may provide harmful effects to a computer. The motivation of Coley et al is that problems in the prior art exist when a packet comprises an unknown address and because it is not identified, it is allowed to pass (col. 3, lines 11-14) and this presents a problem because it provides the hacker a means to bypass the packet filter (col. 3, lines 21-22). Coley et al utilizes the source address information whereby the flow tag information of Decasper et al discloses that the source address is included within the flow (pg 4). The teachings of Decasper et al would have benefitted from the teachings of Coley et al as a means to block unknown packets which are not listed as authorized (approved) or unauthorized (disapproved) and ultimately protect their computer from an attack whereby conventional packet filtering techniques would have allowed the packet to be passed.

Art Unit: 2131

As per claims 4 and 17, Coley et al is relied upon for monitoring incoming IP (connectionless) packets and to determine the validity of the source address (col. 8, lines 1-3 and col. 11, lines 47-48). If the analyzed source address is compared against authorized (approved list) and unauthorized (disapproved list) addresses maintained by a proxy agent (which is stored in a database) and the comparison includes checking if the source is unknown, if it is not on the list, then it is denied (col. 11, lines 22-32).

As per claims 5 and 18, Decasper et al teaches of receiving IPv6 (connectionless) packets which is associated with an identifier (flow tag). If the (connectionless) packet includes an unknown flow, a new flow entry is automatically created (computed) for it which is added to and stored in the AIU (database comprising an approved list) and it is allowed to pass (pg 4 & 5). On pg 4 it is recited that the AIU (database) is used for flow detection which the examiner asserts that incoming identifiers (flow tags) are compared to (approved) data previously stored whereby a match is performed and the IPv6 (connectionless) packet is allowed to pass.

As per claims 6 and 19, the teachings of both Decasper et al and Coley et al are silent in disclosing of recording all allowances of access to the information protection network and recording all discarded connectionless (IP) packets. The examiner hereby takes official notice that such a concept is notoriously well known in the art. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply an event log which records all actions that have occurred whereby specific information is stored by type. It is notoriously well known that logs record various information for use by a user or system

Art Unit: 2131

administrator for later reference in case if the information is desired to be viewed and interpreted. For purposes of auditing, a user or administrator can access the information and analyze the patterns to see the rate of usage to determine the events which led up to a situation such as an attack. Certain packets that are either approved or disapproved would be recorded in the event log and it can be figured out in what manner they have been sent. In the case of Coley et al, this would have been beneficial to the teachings for an attack could have been analyzed so that it could be learned how the attack occurred and future attacks can be detected more easily based on viewing the results as recorded in an event log.

As per claims 7,8,20, and 21, the teachings of both Decasper et al and Coley et al are silent in disclosing of alerting a system administrator if the number of discarded IP packets exceed just a user-definable threshold or a user definable threshold within a user definable span of time. The examiner hereby takes official notice that such a concept is notoriously well known in the art. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to alert an administrator if a threshold is reached over a specific time period. It is notoriously well known that the packet rate of transfers vary based on certain times of the days, whereby there will be peak performance times over certain periods. Allowing a user-definable threshold or a user definable threshold within a user definable span of time would allow the user to determine the effectiveness of triggering an alert to an administrator about the threshold being reached. Certain attacks such as a denial of service attack flood the system with many packets and overwhelm it because all the packets cannot be processed due to exceeding

Art Unit: 2131

capacity. A threshold value would have to be determined which considers normal packet transfers over peak and off-peak hours, but would effectively determine an attack such as a denial of service attack whereby the administrator would be alerted.

***Allowable Subject Matter***

4. Claims 2,3,9-13,15,16, and 22-26 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2131

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Revak whose telephone number is (703) 305-1843. The examiner can normally be reached on Monday-Thursday from 6:30 am to 4:00 pm. The examiner can also be reached on alternate Fridays from 6:30 am to 3:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned as follows:

for After-Final Communications: (703) 746-7238;

for Official Communications: (703) 746-7239;

for Non-Official Communications: (703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

*Gail Hayes*  
GAIL HAYES  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2170

CR

*for*  
June 19, 2003